Constructions of Strongly Regular Cayley Graphs and Skew Hadamard Difference Sets from Cyclotomic Classes

Tao Feng* Koji Momihara† Qing Xiang‡

Abstract

In this paper, we give a construction of strongly regular Cayley graphs and a construction of skew Hadamard difference sets. Both constructions are based on choosing cyclotomic classes in finite fields, and they generalize the constructions given by Feng and Xiang [10, 12]. Three infinite families of strongly regular graphs with new parameters are obtained. The main tools that we employed are index 2 Gauss sums, instead of cyclotomic numbers.

Keywords: Cyclotomic class, Gauss sum, skew Hadamard difference set, strongly regular graph.

1 Introduction

We assume that the reader is familiar with the basic theory of strongly regular graphs and difference sets. For the theory of strongly regular graphs, our main references are the lecture notes of Brouwer and Haemers [5] and [13]. For difference sets, we refer the reader to [17] and Chapter 6 of [2]. We remark that strongly regular graphs are closely related to other combinatorial objects, such as two-weight codes, two-intersection sets in finite geometry, and partial difference sets. For these connections, we refer the reader to [5, p. 132], [7, 22].

Let Γ be a (simple, undirected) graph. The adjacency matrix of Γ is the $(0,1)$-matrix A with both rows and columns indexed by the vertex set of Γ, where $A_{xy} = 1$ when there is an edge between x and y in Γ and $A_{xy} = 0$ otherwise. A useful way to check whether a graph is strongly regular is by using the eigenvalues of its adjacency matrix. For convenience we call an eigenvalue *restricted* if it has an eigenvector perpendicular to the all-ones vector $\mathbf{1}$. (For a k-regular connected graph, the restricted eigenvalues are the eigenvalues different from k.)

Theorem 1.1. *For a simple graph Γ of order v, not complete or edgeless, with adjacency matrix A, the following are equivalent:*

1. *Γ is strongly regular with parameters (v, k, λ, μ) for certain integers k, λ, μ,*

[1]Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, China;
Email: pku.tfeng@yahoo.com.cn
[2]Faculty of Education, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan;
Email: momihara@educ.kumamoto-u.ac.jp
[3]Department of Mathematical Science, University of Delaware, Newark, DE 19716, USA;
Email: xiang@math.udel.edu

2. $A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$ *for certain real numbers* k, λ, μ, *where* I, J *are the identity matrix and the all-ones matrix, respectively,*

3. *A has precisely two distinct restricted eigenvalues.*

One of the most effective methods for constructing strongly regular graphs is by the Cayley graph construction. For example, the Paley graph $\mathrm{P}(q)$ and the Clebsch graph are both Cayley graphs (moreover they are cyclotomic). Let G be an additively written group of order v, and let D be a subset of G such that $0 \notin D$ and $-D = D$, where $-D = \{-d \mid d \in D\}$. The *Cayley graph on* G *with connection set* D, denoted $\mathrm{Cay}(G, D)$, is the graph with the elements of G as vertices; two vertices are adjacent if and only if their difference belongs to D. In the case when $\mathrm{Cay}(G, D)$ is a strongly regular graph, the connection set D is called a (regular) *partial difference set*. The survey of Ma [22] contains much of what is known about partial difference sets and about connections with strongly regular graphs.

A difference set D in an (additively written) finite group G is called *skew Hadamard* if G is the disjoint union of D, $-D$, and $\{0\}$. The primary example (and for many years, the only known example in abelian groups) of skew Hadamard difference sets is the classical Paley difference set in $(\mathbb{F}_q, +)$ consisting of the nonzero squares of $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of order q, and q is a prime power congruent to 3 modulo 4. This situation changed dramatically in recent years. Skew Hadamard difference sets are currently under intensive study; see the introduction of [12] for a short survey of known constructions of skew Hadamard difference sets and related problems.

As we have seen above, in order to obtain strongly regular Cayley graphs, we need to construct regular partial difference sets. A classical method for constructing both partial difference sets and difference sets in the additive groups of finite fields is to use cyclotomic classes of finite fields. Let p be a prime, f a positive integer, and let $q = p^f$. Let $N > 1$ be an integer such that $N|(q-1)$, and γ be a primitive element of $\mathbb{F}_q$. Then the cosets $C_i = \gamma^i \langle \gamma^N \rangle$, $0 \le i \le N-1$, are called the *cyclotomic classes of order* N of $\mathbb{F}_q$. The numbers $|(C_i + 1) \cap C_j|$ are called *cyclotomic numbers*. Many authors have studied the problem of determining when a union of some cyclotomic classes forms a (partial) difference set. A summary of results in this direction obtained up to 1967 appeared in [25]. However, all the results in [25] are based on cyclotomic classes of small orders and this method has had only very limited success. In fact, known infinite series of difference sets were obtained only in the case when $N = 2$. The situation for partial difference sets is slightly better (see [6], [5, p. 137-138]). One of the reasons why very few difference sets have been discovered by this method is the difficulty of computing cyclotomic numbers of order N when N is large. So far cyclotomic numbers have been evaluated for $N \le 24$ [1] (but note that some of these evaluations are not explicit). For large N, probably Van Lint and Schrijver [21] are the first to use cyclotomic classes of order N of finite fields to construct strongly regular graphs, and Baumert, Mills and Ward [4] are the first to use cyclotomic classes of order N of finite fields to construct difference sets. We comment that the difference sets constructed in [4] are also partial difference sets since the finite fields involved have characteristic 2. Both constructions are based on the so-called uniform cyclotomy, which will be defined in Section 2.

On the other hand, many sporadic examples of strongly regular Cayley graphs have been found using unions of cyclotomic classes of $\mathbb{F}_q$ by computer search. For example, the following are known:

(i) (De Lange [20]) Let $q = 2^{12}$ and $N = 45$. Then, $\mathrm{Cay}(\mathbb{F}_q, C_0 \cup C_5 \cup C_{10})$ is a strongly regular graph.

(ii) (Ikuta and Munemasa [15]) Let $q = 2^{20}$ and $N = 75$. Then, $\mathrm{Cay}(\mathbb{F}_q, C_0 \cup C_3 \cup C_6 \cup C_9 \cup C_{12})$ is a strongly regular graph.

(iii) (Ikuta and Munemasa [15]) Let $q = 2^{21}$ and $N = 49$. Then, $\mathrm{Cay}(\mathbb{F}_q, C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6)$ is a strongly regular graph.

Recently, in [10], the first and the third authors extended the above examples to infinite families by using index 2 Gauss sums over $\mathbb{F}_q$. Below is the main theorem from [10].

Theorem 1.2. *(i) Let $p_1 \equiv 3 \pmod 4$ be a prime, $p_1 \neq 3$, $N = p_1^m$, and let p be a prime such that $f := \mathrm{ord}_N(p) = \phi(N)/2$, where ϕ is the Euler totient function. Let $q = p^f$ and $D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i \subseteq \mathbb{F}_q$. Assume that $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph.*

(ii) Let p_1 and p_2 be primes such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $N = p_1^m p_2$, and let p be a prime such that $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2}(p) = \phi(p_2^n)$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and $D = \bigcup_{i=0}^{p_1^{m-1}-1} C_{ip_2} \subseteq \mathbb{F}_q$. Assume that $p_1 = 2p^{h/2} + (-1)^{\frac{p_1-1}{2}} b$, $p_2 = 2p^{h/2} - (-1)^{\frac{p_1-1}{2}} b$, h is even, and $1 + p_1 p_2 = 4p^h$, where $b \in \{1, -1\}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1 p_2})$. Then $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph.

Furthermore, in [12], the following two constructions of skew Hadamard difference sets and Paley type partial difference sets were given. (A partial difference set D in a group G is said to be of *Paley type* if the parameters of the corresponding strongly regular Cayley graph are $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$.)

Theorem 1.3. *(i) Let $p_1 \equiv 7 \pmod 8$ be a prime, $N = 2p_1^m$, and let p be a prime such that $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let s be an odd integer, I any subset of $\mathbb{Z}_N$ such that $\{i \pmod{p_1^m} \mid i \in I\} = \mathbb{Z}_{p_1^m}$, and let $D = \bigcup_{i \in I} C_i \subseteq \mathbb{F}_{p^{fs}}$. Then, D is a skew Hadamard difference set if $p \equiv 3 \pmod 4$ and D is a Paley type partial difference set if $p \equiv 1 \pmod 4$.*

(ii) Let $p_1 \equiv 3 \pmod 8$ be a prime, $p_1 \neq 3$, $N = 2p_1$, and let $p \equiv 3 \pmod 4$ be a prime such that $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, $I = \langle p \rangle \cup 2\langle p \rangle \cup \{0\}$, and let $D = \bigcup_{i \in I} C_i \subseteq \mathbb{F}_q$. Assume that $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then, D is a skew Hadamard difference set in the additive group of $\mathbb{F}_q$.

Note that in Theorem 1.3 (ii), we need to choose a suitable primitive element γ of $\mathbb{F}_q$. For details, see [12]. To extend the construction of Theorem 1.3 (ii) to the general case $N = 2p_1^m$ was left as an open problem in [12].

The purpose of this paper is to generalize the constructions of strongly regular Cayley graphs in Theorem 1.2 (ii) to the case where $N = p_1^m p_2^n$ and of skew Hadamard difference sets in Theorem 1.3 (ii) to the case where $N = 2p_1^m$. Three infinite families of strongly regular graphs with new parameters are obtained (see Table 2 in Section 3). An infinite series of skew Hadamard difference sets in $(\mathbb{F}_q, +)$, where $q = 3^{53 \cdot 107^{m-1}}$, is also obtained. Implications of these results on association schemes will be discussed in Section 4.

2 Index 2 Gauss sums

Let p be a prime, f a positive integer, and $q = p^f$. The canonical additive character ψ of $\mathbb{F}_q$ is defined by

$$\psi\colon \mathbb{F}_q \to \mathbb{C}^*, \qquad \psi(x) = \zeta_p^{\mathrm{Tr}_{q/p}(x)},$$

where $\zeta_p = \exp(\frac{2\pi i}{p})$ and $\mathrm{Tr}_{q/p}$ is the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. For a multiplicative character χ of $\mathbb{F}_q$, we define the *Gauss sum*

$$G(\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x).$$

Below are a few basic properties of Gauss sums [18]:

(i) $G(\chi)\overline{G(\chi)} = q$ if χ is nontrivial;

(ii) $G(\chi^p) = G(\chi)$, where p is the characteristic of $\mathbb{F}_q$;

(iii) $G(\chi^{-1}) = \chi(-1)\overline{G(\chi)}$;

(iv) $G(\chi) = -1$ if χ is trivial.

In general, the explicit evaluation of Gauss sums is a very difficult problem. There are only a few cases where the Gauss sums have been evaluated. The simplest case is the so-called *semi-primitive case* (also referred to as *uniform cyclotomy* or *pure Gauss sum*), where there exists an integer j such that $p^j \equiv -1 \pmod N$, here N is the order of the multiplicative character χ involved. See [1, 4, 7] for the explicit evaluation in this case.

The next interesting case is the index 2 case where the subgroup $\langle p\rangle$ generated by $p \in \mathbb{Z}_N^*$ has index 2 in $\mathbb{Z}_N^*$ and $-1 \notin \langle p\rangle$. In this case, it is known that N can have at most two odd prime divisors. Many authors have investigated this case, see e.g., [3, 19, 23, 24, 27, 28]. In particular, a complete solution to the problem of evaluating Gauss sums in this case was recently given in [27]. The following are the results on evaluation of Gauss sums which we will need in the next section.

Theorem 2.1. *([27], Case B1; Theorem 4.10) Let $N = p_1^m p_2^n$, where m and n are positive integers, p_1 and p_2 are primes such that $p_1 \equiv 1 \pmod 4$ and $p_2 \equiv 3 \pmod 4$. Assume that p is a prime such that $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$, and $[\mathbb{Z}_N^* : \langle p\rangle] = 2$. Let $f = \phi(N)/2$, $q = p^f$, and χ be a multiplicative character of order N of $\mathbb{F}_q$. Then, for $0 \le s \le m-1$ and $0 \le t \le n-1$, we have*

$$\begin{aligned} G(\chi^{p_1^s p_2^t}) &= p^{\frac{f-hp_1^s p_2^t}{2}} \left(\frac{b + c\sqrt{-p_1p_2}}{2}\right)^{p_1^s p_2^t}; \\ G(\chi^{p_1^m p_2^t}) &= -p^{\frac{f}{2}}; \\ G(\chi^{p_1^s p_2^n}) &= p^{\frac{f}{2}}, \end{aligned}$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, and b and c are integers determined by $b, c \not\equiv 0 \pmod p$, $4p^h = b^2 + p_1p_2c^2$, and $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$.

Theorem 2.2. *([27], Case D; Theorem 4.12) Let $N = 2p_1^m$, where $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$ and m is a positive integer. Assume that p is a prime such that $[\mathbb{Z}_N^* : \langle p \rangle] = 2$. Let $f = \phi(N)/2$, $q = p^f$, and χ be a multiplicative character of order N of $\mathbb{F}_q$. Then, for $0 \le t \le m-1$, we have*

$$\begin{aligned} G(\chi^{p_1^t}) &= \begin{cases} (-1)^{\frac{p-1}{2}(m-1)} p^{\frac{f-1}{2} - hp_1^t} \sqrt{p^*} \left(\frac{b + c\sqrt{-p_1}}{2} \right)^{2p_1^t}, & \text{if } p_1 \equiv 3 \pmod 8, \\ (-1)^{\frac{p-1}{2} m} p^{\frac{f-1}{2}} \sqrt{p^*}, & \text{if } p_1 \equiv 7 \pmod 8; \end{cases} \\ G(\chi^{2p_1^t}) &= p^{\frac{f - p_1^t h}{2}} \left(\frac{b + c\sqrt{-p_1}}{2} \right)^{p_1^t}; \\ G(\chi^{p_1^m}) &= (-1)^{\frac{p-1}{2}\frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{p^*}, \end{aligned}$$

where $p^* = (-1)^{\frac{p-1}{2}} p$, h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and b and c are integers determined by $4p^h = b^2 + p_1 c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

Note that Theorem 2.2 above is Theorem 4.12 in [27], whose statement contains several misprints. We corrected those misprints in the above statement.

3 Constructions of strongly regular Cayley graphs and skew Hadamard difference sets

We first recall the following well-known lemma in the theory of difference sets (see e.g., [22, 26]).

Lemma 3.1. *Let $(G, +)$ be an abelian group of odd order v, D a subset of G of size $\frac{v-1}{2}$. Assume that $D \cap -D = \emptyset$ and $0 \notin D$. Then, D is a skew Hadamard difference set in G if and only if*

$$\chi(D) = \frac{-1 \pm \sqrt{-v}}{2}$$

for all nontrivial characters χ of G. On the other hand, assume that $0 \notin D$ and $-D = D$. Then D is a Paley type partial difference set in G if and only if

$$\chi(D) = \frac{-1 \pm \sqrt{v}}{2}$$

for all nontrivial characters χ of G.

Let $q = p^f$, where p is a prime and f a positive integer, and let $C_i = \gamma^i \langle \gamma^N \rangle$, $0 \le i \le N-1$, be the cyclotomic classes of order N of $\mathbb{F}_q$, where γ is a fixed primitive element of $\mathbb{F}_q$. From now on, we will assume that D is a union of cyclotomic classes of order N of $\mathbb{F}_q$. In order to check whether a candidate subset, $D = \bigcup_{i \in I} C_i$, is a partial difference set or a skew Hadamard difference set in $(\mathbb{F}_q, +)$, we will compute the sums $\psi(aD) := \sum_{x \in D} \psi(ax)$ for all $a \in \mathbb{F}_q^*$, where ψ is the canonical additive character of $\mathbb{F}_q$. Note that the sum $\psi(aD)$ can be expressed

as a linear combination of Gauss sums using the orthogonality of characters:

$$\begin{aligned}
\psi(aD) &= \frac{1}{N}\sum_{i\in I}\sum_{x\in\mathbb{F}_q^*}\psi(a\gamma^i x^N)\\
&= \frac{1}{N}\sum_{i\in I}\sum_{x\in\mathbb{F}_q^*}\frac{1}{q-1}\sum_{y\in\mathbb{F}_q^*}\psi(y)\sum_{\chi\in\widehat{\mathbb{F}_q^*}}\chi(a\gamma^i x^N)\overline{\chi(y)}\\
&= \frac{1}{(q-1)N}\sum_{i\in I}\sum_{x\in\mathbb{F}_q^*}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}G(\chi^{-1})\chi(a\gamma^i x^N)\\
&= \frac{1}{(q-1)N}\sum_{i\in I}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}G(\chi^{-1})\chi(a\gamma^i)\sum_{x\in\mathbb{F}_q^*}\chi(x^N)\\
&= \frac{1}{N}\sum_{\chi\in C_0^\perp}G(\chi^{-1})\sum_{i\in I}\chi(a\gamma^i),
\end{aligned}$$

where $\widehat{\mathbb{F}_q^*}$ is the group of multiplicative characters of $\mathbb{F}_q^*$ and $C_0^\perp$ is the subgroup of $\widehat{\mathbb{F}_q^*}$ consisting of all χ which are trivial on C_0.

3.1 Strongly regular graphs from unions of cyclotomic classes of order $N = p_1^m p_2^n$

In this subsection, we assume that $N = p_1^m p_2^n$, where m, n are positive integers, p_1 and p_2 are primes such that $p_1 \equiv 1 \pmod 4$ and $p_2 \equiv 3 \pmod 4$. Furthermore, we assume that p is a prime such that $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$, and $\mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and $C_i = \gamma^i\langle\gamma^N\rangle$, $0 \le i \le N-1$, where $f = \mathrm{ord}_N(p)$ and γ is a fixed primitive element of $\mathbb{F}_q$. Define

$$D = \bigcup_{i=0}^{p_1^{m-1}-1}\bigcup_{j=0}^{p_2^{n-1}-1} C_{p_2^n i + p_1^m j}.$$

It is clear that $D = -D$.

Theorem 3.2. *The size of the set $\{\psi(\gamma^a D) \mid a = 0, 1, \ldots, q-2\}$ is at most five.*

Proof: Let χ_e denote the multiplicative character of order e of $\mathbb{F}_q$ such that $\chi_e(\gamma) = \zeta_e$, where $\zeta_e := \exp(\frac{2\pi i}{e})$. Then $\chi_e^d = \chi_{\frac{e}{d}}$ for any divisor d of e. Note that since D is a union of cyclotomic classes of order N, we have $\{\psi(\gamma^a D) \mid a = 0, 1, \ldots, q-2\} = \{\psi(\gamma^a D) \mid a = 0, 1, \ldots, N-1\}$.

To prove the theorem, it is sufficient to evaluate the sums

$$T_a := N \cdot \psi(\gamma^a D) = \sum_{\ell=0}^{p_1^m p_2^n - 1} G(\chi_{p_1^m p_2^n}^{-\ell}) \sum_{i=0}^{p_1^{m-1}-1}\sum_{j=0}^{p_2^{n-1}-1} \chi_{p_1^m p_2^n}^{\ell}(\gamma^{a+p_2^n i + p_1^m j}),$$

where $a = 0, 1, \ldots, N-1$.

For $\ell = 0$, by noting that $G(\chi_{p_1^m p_2^n}^0) = -1$, we have

$$G(\chi_{p_1^m p_2^n}^0) \sum_{i=0}^{p_1^{m-1}-1}\sum_{j=0}^{p_2^{n-1}-1} \chi_{p_1^m p_2^n}^{\ell}(\gamma^{a+p_2^n i + p_1^m j}) = -p_1^{m-1} p_2^{n-1}.$$

For $\ell = p_1 h$ but $h \not\equiv 0 \pmod{p_1^{m-1}}$, we have

$$\sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^m p_2^n}^{p_1 h}(\gamma^{p_2^n i}) = \sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^{m-1}}^{h}(\gamma^i) = 0.$$

For $\ell = p_2 h$ but $h \not\equiv 0 \pmod{p_2^{n-1}}$, we have

$$\sum_{j=0}^{p_2^{n-1}-1} \chi_{p_1^m p_2^n}^{p_2 h}(\gamma^{p_1^m j}) = \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^{n-1}}^{h}(\gamma^j) = 0.$$

Note that for each $a \in \{0, 1, \ldots, N-1\}$, there is a unique $i \in \{0, 1, \ldots, p_1^{m-1} - 1\}$ such that $p_1^{m-1} \,|\, a + p_2^n i$; we write $a + p_2^n i = p_1^{m-1} i_a$. Define $\delta_{i_a} = 1$ or 0 depending on whether $i_a \equiv 0 \pmod{p_1}$ or not. Similarly, for each $a \in \{0, 1, \ldots, N-1\}$, there is a unique $j \in \{0, 1, \ldots, p_2^{n-1} - 1\}$ such that $p_2^{n-1} \,|\, a + p_1^m j$; we write $a + p_1^m j = p_2^{n-1} j_a$. Define $\delta_{j_a} = 1$ or 0 depending on whether $j_a \equiv 0 \pmod{p_2}$ or not.

For $\ell = p_1^m h$ but $h \not\equiv 0 \pmod{p_2}$, since $G(\chi_{p_2^n}^{-h}) = -p^{\frac{f}{2}}$ by Theorem 2.1, we have

$$\begin{aligned}
& \sum_{h:\gcd(h,p_2)=1} G(\chi_{p_2^n}^{-h}) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^n}^{h}(\gamma^{a+p_2^n i + p_1^m j}) \\
= \; & -p_1^{m-1} p^{\frac{f}{2}} \sum_{x \in \mathbb{Z}_{p_2}^*} \sum_{y=0}^{p_2^{n-1}-1} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^n}^{x+p_2 y}(\gamma^{a+p_1^m j}) \\
= \; & -p_1^{m-1} p_2^{n-1} p^{\frac{f}{2}} \sum_{x \in \mathbb{Z}_{p_2}^*} \chi_{p_2^n}^{x}(\gamma^{j_a}) \\
= \; & -p_1^{m-1} p_2^{n-1} p^{\frac{f}{2}} (p_2 \delta_{j_a} - 1).
\end{aligned}$$

Similarly, for $\ell = p_2^n h$ but $h \not\equiv 0 \pmod{p_1}$, since $G(\chi_{p_1^m}^{-h}) = p^{\frac{f}{2}}$ by Theorem 2.1, we have

$$\sum_{h:\gcd(h,p_1)=1} G(\chi_{p_1^m}^{-h}) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_1^m}^{h}(\gamma^{a+p_2^n i + p_1^m j}) = p_1^{m-1} p_2^{n-1} p^{\frac{f}{2}} (p_1 \delta_{i_a} - 1).$$

For the remaining cases, we consider the sum

$$\sum_{\ell:\gcd(\ell,p_1 p_2)=1} G(\chi_{p_1^m p_2^n}^{-\ell}) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_1^m p_2^n}^{\ell}(\gamma^{a+p_2^n i + p_1^m j}). \tag{3.1}$$

Note that any multiplicative character of order $p_1^m p_2^n$ can be written as $\chi_{p_1^m}^u \chi_{p_2^n}^v$ for some $u \in \mathbb{Z}_{p_1^m}^*$ and $v \in \mathbb{Z}_{p_2^n}^*$. By Theorem 2.1, we have

$$G(\chi_{p_1^m}^{-u} \chi_{p_2^n}^{-v}) = p^{\frac{f-h}{2}} \frac{b + c\eta_1(u)\eta_2(v)\sqrt{-p_1 p_2}}{2},$$

where $b, c \not\equiv 0 \pmod{p}$, $b^2 + p_1p_2c^2 = 4p^h$, $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$, and η_1 and η_2 are the quadratic characters of $\mathbb{F}_{p_1}^*$ and $\mathbb{F}_{p_2}^*$, respectively. Then, the sum (3.1) is rewritten as

$$\begin{aligned}
& p^{\frac{f-h}{2}} \sum_{u\in\mathbb{Z}_{p_1^m}^*} \sum_{v\in\mathbb{Z}_{p_2^n}^*} \frac{b + c\eta_1(u)\eta_2(v)\sqrt{-p_1p_2}}{2} \sum_{i=0}^{p_1^{m-1}-1} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_1^m}^u(\gamma^{a+p_2^n i+p_1^m j})\chi_{p_2^n}^v(\gamma^{a+p_2^n i+p_1^m j}) \\
= \; & \frac{p^{\frac{f-h}{2}} b}{2} \left(\sum_{u\in\mathbb{Z}_{p_1^m}^*} \sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^m}^u(\gamma^{a+p_2^n i}) \right) \left(\sum_{v\in\mathbb{Z}_{p_2^n}^*} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^n}^v(\gamma^{a+p_1^m j}) \right) \qquad (3.2) \\
+ & \frac{p^{\frac{f-h}{2}} c\sqrt{-p_1p_2}}{2} \left(\sum_{u\in\mathbb{Z}_{p_1^m}^*} \eta_1(u) \sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^m}^u(\gamma^{a+p_2^n i}) \right) \left(\sum_{v\in\mathbb{Z}_{p_2^n}^*} \eta_2(v) \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^n}^v(\gamma^{a+p_1^m j}) \right) \qquad (3.3)
\end{aligned}$$

For (3.2), we have

$$\begin{aligned}
& \frac{p^{\frac{f-h}{2}} b}{2} \left(\sum_{u\in\mathbb{Z}_{p_1^m}^*} \sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^m}^u(\gamma^{a+p_2^n i}) \right) \left(\sum_{v\in\mathbb{Z}_{p_2^n}^*} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^n}^v(\gamma^{a+p_1^m j}) \right) \\
= \; & \frac{p^{\frac{f-h}{2}} b}{2} \left(\sum_{x\in\mathbb{Z}_{p_1}^*} \sum_{y=0}^{p_1^{m-1}-1} \sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^m}^{x+p_1y}(\gamma^{a+p_2^n i}) \right) \left(\sum_{x'\in\mathbb{Z}_{p_2}^*} \sum_{y'=0}^{p_2^{n-1}-1} \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^n}^{x'+p_2y'}(\gamma^{a+p_1^m j}) \right) \\
= \; & \frac{p^{\frac{f-h}{2}} b}{2} \left(p_1^{m-1} \sum_{x\in\mathbb{Z}_{p_1}^*} \chi_{p_1}^x(\gamma^{i_a}) \right) \left(p_2^{n-1} \sum_{x'\in\mathbb{Z}_{p_2}^*} \chi_{p_2}^{x'}(\gamma^{j_a}) \right) \\
= \; & \frac{p^{\frac{f-h}{2}} b}{2} p_1^{m-1}p_2^{n-1}(p_1\delta_{i_a} - 1)(p_2\delta_{j_a} - 1).
\end{aligned}$$

Let $G(\eta_i)$, $i = 1, 2$, be the quadratic Gauss sums of $\mathbb{F}_{p_i}$, respectively. It is well known that $G(\eta_i) = \sqrt{(-1)^{(p_i-1)/2}p_i}$ (see [18]). Then, for (3.3), we have

$$\begin{aligned}
& \frac{p^{\frac{f-h}{2}} c\sqrt{-p_1p_2}}{2} \left(\sum_{x\in\mathbb{Z}_{p_1}^*} \sum_{y=0}^{p_1^{m-1}-1} \eta_1(x) \sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^m}^{x+p_1y}(\gamma^{a+p_2^n i}) \right) \left(\sum_{x'\in\mathbb{Z}_{p_2}^*} \sum_{y'=0}^{p_2^{n-1}-1} \eta_2(x') \sum_{j=0}^{p_2^{n-1}-1} \chi_{p_2^n}^{x'+p_2y'}(\gamma^{a+p_1^m j}) \right) \\
= \; & \frac{p^{\frac{f-h}{2}} c\sqrt{-p_1p_2}}{2} \left(p_1^{m-1} \sum_{x\in\mathbb{Z}_{p_1}^*} \eta_1(x)\chi_{p_1}^x(\gamma^{i_a}) \right) \left(p_2^{n-1} \sum_{x'\in\mathbb{Z}_{p_2}^*} \eta_2(x')\chi_{p_2}^{x'}(\gamma^{j_a}) \right) \\
= \; & \frac{p^{\frac{f-h}{2}} c\sqrt{-p_1p_2}}{2} p_1^{m-1}p_2^{n-1}\eta_1(i_a)\eta_2(j_a)G(\eta_1)G(\eta_2) \\
= \; & \frac{p^{\frac{f-h}{2}} c\sqrt{-p_1p_2}}{2} p_1^{m-1}p_2^{n-1}\eta_1(i_a)\eta_2(j_a)\sqrt{(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}}p_1p_2} \\
= \; & -\frac{p^{\frac{f-h}{2}} c}{2} p_1^m p_2^n \eta_1(i_a)\eta_2(j_a).
\end{aligned}$$

Thus, we obtain

$$T_a + p_1^{m-1}p_2^{n-1} = p_1^{m-1}p_2^{n-1}p^{\frac{f}{2}}(-p_2\delta_{j_a} + p_1\delta_{i_a}) + \frac{p^{\frac{f-h}{2}}b}{2}p_1^{m-1}p_2^{n-1}(p_1\delta_{i_a} - 1)(p_2\delta_{j_a} - 1) - \frac{p^{\frac{f-h}{2}}c}{2}p_1^m p_2^n \eta_1(i_a)\eta_2(j_a).$$

Now, we compute $S_a := (T_a + p_1^{m-1}p_2^{n-1})/p_1^{m-1}p_2^{n-1}p^{\frac{f}{2}}$ by considering the following four cases:

(i) If $\delta_{j_a} = \delta_{i_a} = 0$, we have $S_a = \frac{p^{\frac{-h}{2}}b}{2} \pm \frac{p^{\frac{-h}{2}}c}{2}p_1p_2$.

(ii) If $\delta_{j_a} = 1, \delta_{i_a} = 0$, we have $S_a = -p_2 - \frac{p^{\frac{-h}{2}}b}{2}(p_2 - 1)$.

(iii) if $\delta_{j_a} = 0, \delta_{i_a} = 1$, we have $S_a = p_1 - \frac{p^{\frac{-h}{2}}b}{2}(p_1 - 1)$.

(iv) if $\delta_{j_a} = \delta_{i_a} = 1$, we have $S_a = -p_2 + p_1 + \frac{p^{\frac{-h}{2}}b}{2}(p_1 - 1)(p_2 - 1)$.

The proof is now complete. □

Corollary 3.3. *If $b, c \in \{1, -1\}$, h is even, $p_1 = 2p^{h/2} + b$, and $p_2 = 2p^{h/2} - b$, then* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is a strongly regular graph.*

Proof: Since $-D = D$ and $0 \notin D$, the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is undirected and without loops. It is also regular of valency $|D|$. The restricted eigenvalues of this Cayley graph, as explained in [5, p. 134], are $\psi(\gamma^a D)$, where $a = 0, 1, \ldots, q-2$. By Theorem 1.1, it suffices to show that the set $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\}$ has precisely two elements. We substitute $p_1 = 2p^{h/2} + b$, $p_2 = 2p^{h/2} - b$, and $b, c \in \{1, -1\}$ into the expressions for S_a in the proof of Theorem 3.2, and find that S_a indeed take only two distinct values. This proves that $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph. In particular, the two restricted eigenvalues r and s ($r > s$) are given by $r = \frac{2p^{\frac{f+h}{2}} - 1}{p_1p_2}$ and $s = \frac{-2p^{\frac{f+h}{2}} + p^{\frac{f-h}{2}} - 1}{p_1p_2}$, or $s = \frac{-2p^{\frac{f+h}{2}} - 1}{p_1p_2}$ and $r = \frac{2p^{\frac{f+h}{2}} - p^{\frac{f-h}{2}} - 1}{p_1p_2}$ depending on whether $b = 1$ or $b = -1$. Furthermore, the parameters k, λ, and μ of the strongly regular graph are given by $k = \frac{p^f - 1}{p_1p_2}$, $\lambda = s + r + k + sr$, and $\mu = k + sr$. □

Remark 3.4. *One can show that the assumptions on p_1, p_2, b, c, and h are also necessary for* $\mathrm{Cay}(\mathbb{F}_q, D)$ *to be strongly regular by a similar proof to that of Corollary 5.2 in [10].*

The construction of strongly regular Cayley graphs given in this subsection is a generalization of Theorem 1.2 (ii) [10]. In [10], the six infinite series of strongly regular graphs in Table 1 below were obtained. Note that the case when $m = 2$ of the 1st series of Table 1 is the example found by De Lange [20] and the case when $m = 2$ of the 2nd series of Table 1 is the example found by Ikuta and Munemasa [15]. These six infinite series are combined and generalized to three infinite families of strongly regular graphs in Table 2.

Example 3.5. *Table 2 gives generalizations of strongly regular graphs in Table 1. Here, the parameters p, N, h, b satisfy the conditions of Corollary 3.3, i.e., p is a prime such that*

Table 1: Some strongly regular graphs obtained in [10]. The parameters r, s are the two nontrivial eigenvalues of $\mathrm{Cay}(G, D)$, i.e., the two values in $\{\psi(\gamma^a D) \mid a = 0, 1, \ldots, q-2\}$. The parameters λ and μ of the strongly regular graphs can be computed by $\lambda = s + r + sr + k$ and $\mu = k + sr$.

No.	p	N	h	b	v	k	r	s
1	2	$3^m \cdot 5$	2	1	$2^{4\cdot 3^{m-1}}$	$\frac{2^{4\cdot 3^{m-1}}-1}{15}$	$\frac{8\cdot 2^{2\cdot 3^{m-1}-1}-1}{15}$	$\frac{-7\cdot 2^{2\cdot 3^{m-1}-1}-1}{15}$
2	2	$5^m \cdot 3$	2	1	$2^{4\cdot 5^{m-1}}$	$\frac{2^{4\cdot 5^{m-1}}-1}{15}$	$\frac{8\cdot 2^{2\cdot 5^{m-1}-1}-1}{15}$	$\frac{-7\cdot 2^{2\cdot 5^{m-1}-1}-1}{15}$
3	3	$5^m \cdot 7$	2	-1	$3^{12\cdot 5^{m-1}}$	$\frac{3^{12\cdot 5^{m-1}}-1}{35}$	$\frac{17\cdot 3^{6\cdot 5^{m-1}-1}-1}{35}$	$\frac{-18\cdot 3^{6\cdot 5^{m-1}-1}-1}{35}$
4	3	$7^m \cdot 5$	2	-1	$3^{12\cdot 7^{m-1}}$	$\frac{3^{12\cdot 7^{m-1}}-1}{35}$	$\frac{17\cdot 3^{6\cdot 7^{m-1}-1}-1}{35}$	$\frac{-18\cdot 3^{6\cdot 7^{m-1}-1}-1}{35}$
5	3	$17^m \cdot 19$	4	-1	$3^{144\cdot 17^{m-1}}$	$\frac{3^{144\cdot 17^{m-1}}-1}{323}$	$\frac{161\cdot 3^{72\cdot 17^{m-1}-2}-1}{323}$	$\frac{-162\cdot 3^{72\cdot 17^{m-1}-2}-1}{323}$
6	3	$19^m \cdot 17$	4	-1	$3^{144\cdot 19^{m-1}}$	$\frac{3^{144\cdot 19^{m-1}}-1}{323}$	$\frac{161\cdot 3^{72\cdot 17^{m-1}-2}-1}{323}$	$\frac{-162\cdot 3^{72\cdot 17^{m-1}-2}-1}{323}$

$[\mathbb{Z}_N^* : \langle p \rangle] = 2$, $b, c \in \{1, -1\}$, $p_1 = 2p^{h/2} + b$, $p_2 = 2p^{h/2} - b$, $h \equiv 0 \pmod 2$, and $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1 p_2}$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1 p_2})$. It is easy to see by induction that $\mathrm{ord}_N(p) = \phi(N)/2$ for all pairs (p, N) in Table 2. Furthermore, since $(p^{p_1^{m-1} p_2^{n-1}})^{\frac{p_1-1}{2}\frac{p_2-1}{2}} \equiv p^{\frac{p_1-1}{2}\frac{p_2-1}{2}} \pmod{p_1 p_2}$, the condition $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1 p_2}$ can be rewritten as $bp^{\frac{p_1-1}{2}\frac{p_2-1}{2}} \equiv 2p^{\frac{h}{2}} \pmod{p_1 p_2}$, which is independent of m and n. There are only these three series satisfying the conditions of Corollary 3.3 when $p_1 \le 10^7$.

Table 2: Generalizations of the strongly regular graphs in Table 1. The parameters λ and μ of the strongly regular graphs can be computed by $\lambda = s + r + sr + k$ and $\mu = k + sr$.

No.	p	N	h	b	v	k	r, s
7	2	$3^m \cdot 5^n$	2	1	$2^{4\cdot 3^{m-1}\cdot 5^{n-1}}$	$\frac{2^{4\cdot 3^{m-1}\cdot 5^{n-1}}-1}{15}$	$r = \frac{8\cdot 2^{2\cdot 3^{m-1}\cdot 5^{n-1}-1}-1}{15}$ $s = \frac{-7\cdot 2^{2\cdot 3^{m-1}\cdot 5^{n-1}-1}-1}{15}$
8	3	$5^m \cdot 7^n$	2	-1	$3^{12\cdot 5^{m-1}\cdot 7^{n-1}}$	$\frac{3^{12\cdot 5^{m-1}\cdot 7^{n-1}}-1}{35}$	$r = \frac{17\cdot 3^{6\cdot 5^{m-1}\cdot 7^{n-1}-1}-1}{35}$ $s = \frac{-18\cdot 3^{6\cdot 5^{m-1}\cdot 7^{n-1}-1}-1}{35}$
9	3	$17^m \cdot 19^n$	4	-1	$3^{144\cdot 17^{m-1}\cdot 19^{n-1}}$	$\frac{3^{144\cdot 17^{m-1}\cdot 19^{n-1}}-1}{323}$	$r = \frac{161\cdot 3^{72\cdot 17^{m-1}\cdot 19^{n-1}-2}-1}{323}$ $s = \frac{-162\cdot 3^{72\cdot 17^{m-1}\cdot 19^{n-1}-2}-1}{323}$

3.2 Skew Hadamard difference sets from unions of cyclotomic classes of order $N = 2p_1^m$

In this subsection, we assume that

1. $p_1 \equiv 3 \pmod 8$, $(p_1 \neq 3)$,
2. $N = 2p_1^m$,
3. $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$,
4. p is a prime such that $\mathrm{ord}_N(p) = \phi(p_1^m)/2$.

Let $q = p^f$, where $f = \mathrm{ord}_N(p)$. Let $\zeta_{q-1} = \exp(\frac{2\pi i}{q-1})$ and $\mathfrak{P}$ be a prime ideal in $\mathbb{Z}[\zeta_{q-1}]$ lying over p. Then, $\mathbb{Z}[\zeta_{q-1}]/\mathfrak{P}$ is the finite field of order q and written as $\mathbb{Z}[\zeta_{q-1}]/\mathfrak{P} = \{\overline{\zeta}_{q-1}^i \,|\, 0 \leq i \leq q-2\} \cup \{\overline{0}\}$, where $\overline{\zeta}_{q-1} = \zeta_{q-1} + \mathfrak{P}$. Hence, $\gamma := \overline{\zeta}_{q-1}$ is a primitive element of $\mathbb{F}_q = \mathbb{Z}[\zeta_{q-1}]/\mathfrak{P}$. Let $\omega_{\mathfrak{P}}$ be the Teichmüller character of $\mathbb{F}_q$. Then, $\omega_{\mathfrak{P}}(\gamma) = \zeta_{q-1}$. Put $\chi_N := \omega_{\mathfrak{P}}^{\frac{q-1}{N}}$. Then χ_N is a multiplicative character of order N of $\mathbb{F}_q$. For this χ_N, by the results of [19], we have

$$G(\chi_N^2) = G(\chi_{p_1^m}) = p^{\frac{f-h}{2}} \left(\frac{b + c\sqrt{-p_1}}{2} \right), \tag{3.4}$$

where $b, c \not\equiv 0 \pmod p$, $b^2 + c^2 p_1 = 4p^h$, and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$. By our assumption that $1 + p_1 = 4p^h$, we have $b, c \in \{-1, 1\}$, where the sign of c depends on the choice of $\mathfrak{P}$. In particular, in [12], it was shown that $bc \equiv -\sqrt{-p_1} \pmod{\mathfrak{P}}$. On the other hand, since $1 + p_1 = 4p^h$, we have $(1 + \sqrt{-p_1})(1 - \sqrt{-p_1}) \in \mathfrak{P}$, from which it follows that $1 + \sqrt{-p_1} \in \mathfrak{P}$ or $1 - \sqrt{-p_1} \in \mathfrak{P}$ for any prime ideal $\mathfrak{P}$ in $\mathbb{Q}(\zeta_{q-1})$ lying over p. We may choose a prime ideal $\mathfrak{P}$ such that $1 + \sqrt{-p_1} \in \mathfrak{P}$. Then, $bc \equiv -\sqrt{-p_1} \pmod{\mathfrak{P}}$ with $b, c \in \{-1, 1\}$ implies that $bc = 1$. From now on, we fix this choice of $\mathfrak{P}$.

Let $C_i = \gamma^i \langle \gamma^N \rangle$, where $0 \leq i \leq N-1$, and γ is the fixed primitive element of $\mathbb{F}_q$ as above. It is clear that $-1 \in C_0$ or $-1 \in C_{p_1^m}$ depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

Let

$$J = \langle p \rangle \cup 2\langle p \rangle \cup \{0\} \pmod{2p_1}$$

and define

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j \in J} C_{2i + p_1^{m-1} j}.$$

From the facts that 2 is a nonsquare of $\mathbb{F}_{p_1}$ and that the reduction of $\langle p \rangle \leq \mathbb{Z}_N^*$ modulo $2p_1$ is the subgroup of index 2 of $\mathbb{Z}_{2p_1}^*$ we deduce that $J \pmod{p_1} = \mathbb{Z}_{p_1}$, and $D = -D$ or $D \cap -D = \emptyset$ depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

Theorem 3.6. *The size of the set $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\}$ is precisely two.*

Proof: Set $A := (-1)^{\frac{p-1}{2}(m-1)} p^{\frac{f-1}{2}-h} \sqrt{p^*}$ and $B := (-1)^{\frac{p-1}{2}\frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{p^*}$, where $\sqrt{p^*} = \sqrt{(-1)^{\frac{p-1}{2}} p}$.

First of all, we note that $(-1)^{\frac{f-1}{2}} = (-1)^{m-1}$ since $p_1 \equiv 3 \pmod 8$. It follows that $p^h A = B$.

Secondly, since D is a union of cyclotomic classes of order N, we have $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\} = \{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, N-1\}$.

It is sufficient to evaluate the sums

$$T_a := N \cdot \psi(\gamma^a D) = \sum_{\ell=0}^{2p_1^m-1} G(\chi_{2p_1^m}^{\ell}) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{-\ell}(\gamma^{a+2i+p_1^{m-1}j}),$$

where $a = 0, 1, \ldots, N-1$.

For $\ell = 0$, by noting that $G(\chi_{2p_1^m}^0) = -1$, we have

$$G(\chi_{2p_1^m}^0) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^0(\gamma^{a+2i+p_1^{m-1}j}) = -p_1^m.$$

For $\ell = 2h$ but $h \not\equiv 0 \pmod{p_1}$, since $J \pmod{p_1} = \mathbb{Z}_{p_1}$, we have

$$\sum_{j\in J} \chi_{2p_1^m}^{-2h}(\gamma^{p_1^{m-1}j}) = \sum_{j\in J} \chi_{p_1}^{-h}(\gamma^j) = 0.$$

For $\ell = p_1 h$ but $h \not\equiv 0 \pmod{p_1^{m-1}}$, we have

$$\sum_{i=0}^{p_1^{m-1}-1} \chi_{2p_1^m}^{-p_1 h}(\gamma^{2i}) = \sum_{i=0}^{p_1^{m-1}-1} \chi_{p_1^{m-1}}^{-h}(\gamma^i) = 0.$$

For $\ell = p_1^m$, since $G(\chi_{2p_1^m}^{p_1^m}) = B$ by Theorem 2.2, we have

$$G(\chi_{2p_1^m}^{p_1^m}) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{p_1^m}(\gamma^{a+2i+p_1^{m-1}j}) = Bp_1^{m-1}(-1)^a.$$

For the remaining cases, we evaluate the sum

$$\sum_{\ell\in\langle p\rangle} G(\chi_{2p_1^m}^{\ell}) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{-\ell}(\gamma^{a+2i+p_1^{m-1}j}) + \sum_{\ell\in -\langle p\rangle} G(\chi_{2p_1^m}^{\ell}) \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{-\ell}(\gamma^{a+2i+p_1^{m-1}j}).$$

By Theorem 2.2, we have

$$G(\chi_{2p_1^m}^{\ell}) = A\left(\frac{b + c\sqrt{-p_1}}{2}\right)^2$$

for $\ell \in \langle p\rangle$, where b, c are the same as in the evaluation (3.4) of $G(\chi_{p_1^m})$. By the choice of $\mathfrak{P}$, it is expanded as

$$G(\chi_{2p_1^m}^{\ell}) = A\left(\frac{1 - p_1 + 2\sqrt{-p_1}}{4}\right).$$

Since $\chi_{2p_1^m}^{\ell}(-1)\overline{\sqrt{p^*}} = \sqrt{p^*}$ for any odd ℓ by the assumption $p_1 \equiv 3 \pmod 8$, i.e., f is odd, the above sum is reformulated as

$$A\left(\frac{1 - p_1 + 2\sqrt{-p_1}}{4}\right) \sum_{\ell\in\langle p\rangle} \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{-\ell}(\gamma^{a+2i+p_1^{m-1}j})$$

$$+A\left(\frac{1 - p_1 - 2\sqrt{-p_1}}{4}\right) \sum_{\ell\in -\langle p\rangle} \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{-\ell}(\gamma^{a+2i+p_1^{m-1}j}).$$

Note that $\langle p\rangle$ can be written as $\{x+2p_1y \,|\, x \in \langle p\rangle (\mathrm{mod}\ 2p_1), y \in \{0,1,\ldots,p_1^{m-1}-1\}\}$. Furthermore, there is a unique $i \in \{0,1,\ldots,p_1^{m-1}-1\}$ such that $a+2i \equiv 0 \,(\mathrm{mod}\ p_1^{m-1})$; we write $a+2i = p_1^{m-1}i_a$. Then, the above sum is rewritten as

$$\begin{aligned}
& A\left(\frac{1-p_1+2\sqrt{-p_1}}{4}\right) \sum_{x\in\langle p\rangle (\mathrm{mod}\ 2p_1)} \sum_{y=0}^{p_1^{m-1}-1} \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{-x}(\gamma^{a+2i+p_1^{m-1}j}) \chi_{2p_1^m}^{-2p_1y}(\gamma^{a+2i+p_1^{m-1}j}) \\
& \quad + A\left(\frac{1-p_1-2\sqrt{-p_1}}{4}\right) \sum_{x\in-\langle p\rangle (\mathrm{mod}\ 2p_1)} \sum_{y=0}^{p_1^{m-1}-1} \sum_{i=0}^{p_1^{m-1}-1} \sum_{j\in J} \chi_{2p_1^m}^{-x}(\gamma^{a+2i+p_1^{m-1}j}) \chi_{2p_1^m}^{-2p_1y}(\gamma^{a+2i+p_1^{m-1}j}) \\
= \ & p_1^{m-1} A\left(\frac{1-p_1+2\sqrt{-p_1}}{4}\right) \sum_{x\in\langle p\rangle (\mathrm{mod}\ 2p_1)} \sum_{j\in J} \chi_{2p_1}^{-x}(\gamma^{i_a+j}) \\
& \quad + p^{m-1} A\left(\frac{1-p_1-2\sqrt{-p_1}}{4}\right) \sum_{x\in-\langle p\rangle (\mathrm{mod}\ 2p_1)} \sum_{j\in J} \chi_{2p_1}^{-x}(\gamma^{i_a+j}) \\
= \ & p_1^{m-1} A\left(\frac{1-p_1+2\sqrt{-p_1}}{4}\right) \left(\sum_{x\in\langle p\rangle (\mathrm{mod}\ 2p_1)} \chi_{2p_1}^{-x}(\gamma^{i_a})\right) \left(\sum_{j\in J} \chi_{2p_1}^{-j}(\gamma)\right) \\
& \quad + p^{m-1} A\left(\frac{1-p_1-2\sqrt{-p_1}}{4}\right) \left(\sum_{x\in\langle p\rangle (\mathrm{mod}\ 2p_1)} \chi_{2p_1}^{x}(\gamma^{i_a})\right) \left(\sum_{j\in J} \chi_{2p_1}^{j}(\gamma)\right).
\end{aligned}$$

Put $X_a := \sum_{j\in J} \chi_{2p_1}^{-j}(\gamma)$ and $Y_a := \sum_{x\in\langle p\rangle (\mathrm{mod}\ 2p_1)} \chi_{2p_1}^{-x}(\gamma^{i_a})$. Let η be the quadratic character of $\mathbb{F}_{p_1}$ and ψ_{p_1} be the canonical additive character of $\mathbb{F}_{p_1}$. Noting that 2 is a nonsquare in $\mathbb{F}_{p_1}$. For $i \in \mathbb{Z}_{2p_1} \setminus \{0, p_1\}$ it holds that

$$\begin{aligned}
\sum_{x\in\langle p\rangle (\mathrm{mod}\ 2p_1)} \chi_{2p_1}^{-x}(\gamma^i) &= \sum_{x\in\langle p\rangle (\mathrm{mod}\ 2p_1)} \chi_2^{-ix}(\gamma) \chi_{p_1}^{\frac{p_1-1}{2}ix}(\gamma) \\
&= (-1)^i \frac{1}{2} \sum_{x\in\mathbb{F}_{p_1}^*} (1+\eta(x)) \psi_{p_1}(-2^{-1}ix) \\
&= (-1)^i \frac{-1+\eta(-2^{-1}i)G(\eta)}{2} = (-1)^i \frac{-1+\eta(i)\sqrt{-p_1}}{2}.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
X_a &= \sum_{j\in\langle p\rangle \,(\mathrm{mod}\ 2p_1)} \chi_{2p_1}^{-j}(\gamma) + \sum_{j\in 2\langle p\rangle \,(\mathrm{mod}\ 2p_1)} \chi_{2p_1}^{-j}(\gamma) + 1 \\
&= \frac{1-\sqrt{-p_1}}{2} + \frac{-1-\sqrt{-p_1}}{2} + 1 = 1-\sqrt{-p_1}
\end{aligned}$$

and

$$Y_a = (-1)^{i_a} \frac{-1+\eta(i_a)\sqrt{-p_1}}{2},\ i_a \neq 0, p_1.$$

Thus, we obtain

$$\begin{aligned}
& T_a + p_1^m \\
= \ & Bp_1^{m-1}(-1)^a + \frac{p_1^{m-1}A}{4}\left((1-p_1+2\sqrt{-p_1})(1-\sqrt{-p_1})Y_a + (1-p_1-2\sqrt{-p_1})(1+\sqrt{-p_1})\overline{Y_a}\right).
\end{aligned}$$

We compute $T_a + p_1^m$ by considering the following six cases:

(i) $i_a = 0$: In this case, we have $a \equiv 0 \pmod 2$, $Y_a = \frac{p_1-1}{2}$, and $T_a + p_1^m = p_1^{m-1}(\frac{A}{4}(p_1^2 - 1) + B)$.

(ii) $i_a = p_1$: In this case, we have $a \equiv 1 \pmod 2$, $Y_a = -\frac{p_1-1}{2}$, and $T_a + p_1^m = p_1^{m-1}(\frac{A}{4}(-p_1^2 + 1) - B)$.

(iii) $i_a \in \langle p \rangle$: In this case, we have $a \equiv 1 \pmod 2$, $Y_a = \frac{1-\sqrt{-p_1}}{2}$, and $T_a + p_1^m = p_1^{m-1}(\frac{A}{4}(p_1^2 + 2p_1 + 1) - B)$.

(iv) $i_a \in -\langle p \rangle$: In this case, we have $a \equiv 1 \pmod 2$, $Y_a = \frac{1+\sqrt{-p_1}}{2}$, and $T_a + p_1^m = p_1^{m-1}(\frac{A}{4}(1 - p_1^2) - B)$.

(v) $i_a \in 2\langle p \rangle$: In this case, we have $a \equiv 0 \pmod 2$, $Y_a = -\frac{1+\sqrt{-p_1}}{2}$, and $T_a + p_1^m = p_1^{m-1}(\frac{A}{4}(p_1^2 - 1) + B)$.

(vi) $i_a \in -2\langle p \rangle$: In this case, we have $a \equiv 0 \pmod 2$, $Y_a = \frac{-1+\sqrt{-p_1}}{2}$, and $T_a + p_1^m = p_1^{m-1}(\frac{A}{4}(-p_1^2 - 2p_1 - 1) + B)$.

By the assumption that $1 + p_1 = 4p^h$ and the fact that $p^h A = B$, it is easily checked that $T_a + p_1^m$, $a = 0, 1, \ldots, N-1$, take precisely two values. The proof is now complete. □

Corollary 3.7. *The set D is a skew Hadamard difference set or a Paley type partial difference set according as $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 4$.*

Proof: By Theorem 3.6, the set $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\}$ has precisely two elements, which are

$$\frac{1}{N}\left(-p_1^m \pm p_1^{m-1}\left(\frac{A}{4}(p_1^2 - 1) + B\right)\right) = \frac{1}{2}\left(-1 \pm (-1)^{\frac{(p-1)(m-1)}{2}}\sqrt{(-1)^{\frac{p-1}{2}}p^f}\right).$$

By Lemma 3.1, the assertion of the corollary follows immediately. □

The construction of skew Hadamard difference sets and Paley type partial difference sets given in this subsection is a generalization of Theorem 1.3 (ii) [12]. In particular, in [12], one example of skew Hadamard difference sets with parameters $(p, N, h, b, v) = (3, 2 \cdot 11, 1, 1, 3^5)$ was given. Unfortunately, we can not generalize this example to $N = 2 \cdot 11^m$ because $p = 3$ does not satisfy the condition $\mathrm{ord}_N(p) = \phi(N)/2$ for $m > 1$. Below are some infinite series of skew Hadamard difference sets and Paley type partial difference sets obtained by Corollary 3.7.

Example 3.8. *Table 3 shows all possible skew Hadamard difference sets and Paley type partial difference sets obtained by applying Corollary 3.7 to all $p_1 \le 10^6$ except for the case when $p_1 = 11$ and $m = 1$. In particular, the 3rd case of Table 3 gives skew Hadamard difference sets and the other cases give Paley type partial difference sets. Here, the parameters p, N, h, b satisfy the conditions of Corollary 3.7, i.e., p is a prime such that $[\mathbb{Z}_N^* : \langle p \rangle] = 2$, $1 + p_1 = 4p^h$, and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Note that it is easy to prove by induction that $\mathrm{ord}_N(p) = \phi(N)/2$ for all pairs (p, N) in Table 3. Furthermore, since*

$$p^{\frac{p_1^{m-1}(p_1-1)/2-h}{2}} \equiv p^{\frac{p_1^{m-1}(p_1+1)}{4} - \frac{p_1^{m-1}-1}{2} - \frac{h+1}{2}} \pmod{p_1},$$

the condition $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$ can be rewritten as $bp^{\frac{p_1-1-2h}{4}} \equiv -2 \pmod{p_1}$, which is independent of m.

Table 3: Some Paley type partial difference sets and skew Hadamard difference sets obtained by Corollary 3.7.

No.	p	N	h	b	v
1	5	$2 \cdot 19^m$	1	1	$5^{9 \cdot 19^{m-1}}$
2	17	$2 \cdot 67^m$	1	1	$17^{33 \cdot 67^{m-1}}$
3	3	$2 \cdot 107^m$	3	1	$3^{53 \cdot 107^{m-1}}$
4	41	$2 \cdot 163^m$	1	1	$41^{81 \cdot 163^{m-1}}$
5	5	$2 \cdot 499^m$	3	1	$5^{249 \cdot 499^{m-1}}$

4 Concluding remarks

In this paper, we have given two constructions of strongly regular graphs and skew Hadamard difference sets, which are generalizations of those given by the first and third authors [10, 12]. As a consequence, we obtain three infinite series of strongly regular graphs with new parameters and a family of skew Hadamard difference sets in $(\mathbb{F}_q, +)$, where $q = 3^{53 \cdot 107^{m-1}}$. The results on strongly regular graphs have implications on association schemes.

Given a d-class (symmetric) association scheme $(X, \{R_\ell\}_{0 \le \ell \le d})$, we can take the union of classes to form graphs with larger edge sets (this process is called a *fusion*), but it is not necessarily guaranteed that the fused collection of graphs will form an association scheme on X. If an association scheme has the property that any of its fusions is also an association scheme, then we call the association scheme *amorphic*. A well-known and important example of amorphic association schemes is given by the cyclotomic association schemes on $\mathbb{F}_q$ when the cyclotomy is uniform [4].

In [16], A.V. Ivanov conjectured that if each nontrivial relation in an association scheme is strongly regular, then the association scheme must be amorphic. This conjecture turned out to be false. A first counterexample was found by Van Dam [8] in the case when the association scheme is imprimitive. Afterwards, Van Dam [9] and Ikuta and Munemasa [15] gave more counterexamples in the case when the association scheme is primitive. However, there had been known only a few counterexamples in the primitive case. Recently, in [11], the authors generalized the counterexamples of Van Dam and Ikuta-Munemasa into infinite series using strongly regular Cayley graphs based on index 2 Gauss sums of type $N = p_1^m$ and type $N = p_1^m p_2$. Our generalization (Corollary 3.3) of the second construction in [10] produces further new counterexamples to Ivanov's conjecture and association schemes with very interesting properties. More precisely, under the same assumptions as in Corollary 3.3, define

$$D_k = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j=0}^{p_2^{n-1}-1} C_{p_2^n i + p_1^m j + p_1^{m-1} p_2^{n-1} k}$$

for each $0 \le k \le p_1 p_2 - 1$. Let $R_0 = \{(x, x) \,|\, x \in \mathbb{F}_q\}$ and

$$R_k := \{(x, y) \,|\, x, y \in \mathbb{F}_q, x - y \in D_{k-1}\}.$$

Then, one can similarly prove that $(\mathbb{F}_q, \{R_k\}_{0\le k\le p_1p_2})$ is a pseudocyclic and non-amorphic association scheme in which every nontrivial relation is a strongly regular graph. Table 2 yields three new infinite series of pseudocyclic and non-amorphic association schemes, where each of the nontrivial relations is strongly regular. Moreover, further fusion schemes of these association schemes are possible by applying Corollary 3.2 and Theorem 4.1 of [15]. In particular, Examples 1 and 2 of [15] are generalized into an infinite series by using the above association scheme with $p = 2$, $b = 1$, $(p_1, p_2) = (5, 3)$, and $h = 2$.

Acknowledgements

The work of Tao Feng was supported in part by the Fundamental Research Funds for the central universities. The work of K. Momihara was supported by JSPS under Grant-in-Aid for Research Activity start-up 23840032. The work of Qing Xiang was supported in part by NSF Grant DMS 1001557 and by the Y. C. Tang disciplinary development fund of Zhejiang University.

References

[1] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.

[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*. Vol. I. Second edition. Encyclopedia of Mathematics and its Applications, 78. Cambridge University Press, Cambridge, 1999.

[3] L. D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, *DSN Progr. Rep.,* **16** (1973), 128–131.

[4] L. D. Baumert, W.H. Mills, R.L. Ward, Uniform cyclotomy, *J. Number Theory*, **14** (1982), 67–82.

[5] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, course notes, available at `http://homepages.cwi.nl/~ aeb/math/ipm.pdf`

[6] A. E. Brouwer, R. M. Wilson, Q. Xiang, Cyclotomy and strongly regular graphs, *J. Alg. Combin.,* **10** (1999), 25–28.

[7] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.,* **18** (1986), 97–122.

[8] E.R. van Dam, A characterization of association schemes from affine spaces, *Des. Codes Cryptogr.,* **21** (2000), 83–86.

[9] E.R. van Dam, Strongly regular decompositions of the complete graphs, *J. Alg. Combin.,* **17** (2003), 181–201.

[10] T. Feng, Q. Xiang, Strongly regular graphs from union of cyclotomic classes, to appear in J. Combin. Theory (B). Available at `arXiv:1010.4107v3`.

[11] T. Feng, F. Wu, Q. Xiang, Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes, to appear in Des, Codes Cryptogr.. Available at `arXiv:1012.2181v2`.

[12] T. Feng, Q. Xiang, Cyclotomic constructions of skew Hadamard difference sets, *J. Combin. Theory* (A), **119** (2012), 245–256.

[13] C. Godsil, G. Royle, *Algebraic Graph Theory*, GTM 207, Springer-Verlag, 2001.

[14] M. Hall, Jr., A survey of difference sets, *Proc. Amer. Math. Soc.,* **7** (1956), 975–986.

[15] T. Ikuta, A. Munemasa, Pseudocyclic association schemes and strongly regular graphs, *Europ. J. Combin.,* **31** (2010), pp. 1513–1519.

[16] A. A. Ivanov, C.E. Praeger, Problem session at ALCOM-91, *Europ. J. Combin.,* **15** (1994), 105–112.

[17] E. S. Lander, *Symmetric designs: an algebraic approach*, Cambridge University Press, 1983.

[18] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.

[19] P. Langevin, Calcus de certaines sommes de Gauss, *J. Number Theory*, **63** (1997), 59–64.

[20] C. L. M. de Lange, Some new cyclotomic strongly regular graphs, *J. Alg. Combin.,* **4** (1995), 329–330.

[21] J. H. van Lint, A. Schrijver, Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica,* **1** (1981), 63–73.

[22] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.,* **4** (1994), 221–261.

[23] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields Appl.,* **4** (1998), 347–361.

[24] P. Meijer, M. van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, *J. Number Theory*, **100** (2003), 381–395.

[25] T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, Markham Publishing Company, 1967.

[26] R. J. Turyn, Character sums and difference sets, *Pacific J. Math.,* **15** (1965), 319–346.

[27] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A*, **53** (2010), 2525–2542.

[28] J. Yang, L. Xia, A note on the sign (unit root) ambiguities of Gauss sums in the index 2 and 4 case, preprint, `arXiv:0912.1414v1`.